

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- a²
1. (Canceled)
 2. (Canceled)
 3. (Currently Amended) ~~The method as recited in claim 2,~~ A method for analyzing a logfile produced by a computer network security system, comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

wherein the pattern is associated with a possible sgid exploit and using the query to search for the pattern includes searching for entries showing that a process has been started with effective group ID equal to zero.

4. (Original) The method as recited in claim 3, wherein using the query to search for the pattern further includes storing a process ID of the process, and searching for processes with a parent process ID equal to the stored process ID.

5. (Canceled)

6. (Currently Amended) ~~The method as recited in claim 5,~~ A method for analyzing a logfile produced by a computer network security system, comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

wherein the pattern is associated with a possible *suid* exploit and using the query to search for the pattern includes searching for entries showing that a process has been started with effective user ID equal to zero.

2²
7. (Original) The method as recited in claim 6, wherein using the query to search for the pattern further includes storing a process ID of the process, and searching for processes with a parent process ID equal to the stored process ID.

8. (Canceled)

9. (Currently Amended) ~~The method as recited in claim 8,~~ A method for analyzing a logfile produced by a computer network security system, comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

wherein the pattern is associated with a possible *sgid* exploit, the pattern is associated with processes spawned by a shell, and using the query to search for the pattern includes searching for entries showing that the shell has started a process, storing a process ID of the process, and searching for entries showing processes with parent process ID equal to the stored process ID.

10. (Canceled)

11. (Canceled)

12. (Canceled)

13. (Currently Amended) ~~The method as recited in claim 2,~~ A method for analyzing a logfile produced by a computer network security system, comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

a² wherein the pattern is associated with a possible sgid exploit, the pattern is associated with screen output characters, and the method further comprises aggregating the screen output characters found in the logfile.

14. (Original) The method as recited in claim 13, wherein the found screen output characters are aggregated upon finding a screen output character representing a newline character.

15. (Original) The method as recited in claim 14, further comprising presenting the aggregated keystrokes to a second user.

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Currently Amended) ~~The method as recited in claim 19, further comprising~~ A method for analyzing a logfile produced by a computer network security system, comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile;

using the query to search for the pattern in the logfile, including by searching for entries showing that a monitored file has been accessed,

indicating to a second user a process ID of a process that accessed the monitored file; and

automatically searching for the process ID in the logfile;

wherein the pattern is associated with a possible *sgid* exploit.

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (Canceled)

29. (Currently Amended) ~~The system as recited in claim 28,~~ A system for analyzing a logfile produced by a computer network security system, comprising:

a storage including a regular expression query associated with a pattern to be searched for in the logfile; and

a processor configured to use the query to search for the pattern in the logfile;

wherein the pattern is associated with a possible *sgid* exploit and the processor is further configured to search for entries showing that a process has been started with effective group ID equal to zero.

30. (Original) The system as recited in claim 29, wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.

31. (Canceled)

32. (Currently Amended) ~~The system as recited in claim 31,~~ A system for analyzing a logfile produced by a computer network security system, comprising:

a storage including a regular expression query associated with a pattern to be searched for in the logfile; and

a processor configured to use the query to search for the pattern in the logfile;

wherein the pattern is associated with a possible *suid* exploit and the processor is further configured to search for entries showing that a process has been started with effective user ID equal to zero.

33. (Original) The system as recited in claim 32, wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.

34. (Canceled)

35. (Currently Amended) A computer program product for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

wherein the pattern is associated with a possible *sgid* exploit and using the query to search for the pattern includes searching for entries showing that a process has been started with effective group ID equal to zero.

36. (Canceled)

37. (New) A computer program product for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for:

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

wherein the pattern is associated with a possible *suid* exploit and using the query to search for the pattern includes searching for entries showing that a process has been started with effective user ID equal to zero.

38. (New) A system for analyzing a logfile produced by a computer network security system, comprising:

a storage including a regular expression query associated with a pattern to be searched for in the logfile; and

a processor configured to use the query to search for the pattern in the logfile;

wherein the pattern is associated with a possible *sgid* exploit, the pattern is associated with screen output characters, and the method further comprises aggregating the screen output characters found in the logfile.

39. (New) A computer program product for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for:

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

a² wherein the pattern is associated with a possible *sgid* exploit, the pattern is associated with screen output characters, and the method further comprises aggregating the screen output characters found in the logfile.

40. (New) A system for analyzing a logfile produced by a computer network security system, comprising:

a storage including a regular expression query associated with a pattern to be searched for in the logfile; and

a processor configured to:

use the query to search for the pattern in the logfile, including by searching for entries showing that a monitored file has been accessed,

indicate to a second user a process ID of a process that accessed the monitored file; and

automatically search for the process ID in the logfile;

wherein the pattern is associated with a possible *sgid* exploit.

41. (New) A computer program product for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for:

providing a regular expression query associated with a pattern to be searched for in the logfile;

using the query to search for the pattern in the logfile, including by searching for entries showing that a monitored file has been accessed,

indicating to a second user a process ID of a process that accessed the monitored file; and

automatically searching for the process ID in the logfile;

wherein the pattern is associated with a possible *sgid* exploit.
